# United States Antarctic Program
Information Security
Computer Screening Requirements

Raytheon Polar Services

The U.S. Federal government requires security and operational practices for computing systems in all government funded programs. The United States Antarctic Program's (USAP) compliance with this federal requirement entails the screening of all computers prior to connecting to the USAP network (wired or wireless). The following requirements apply to personal and business equipment that will connect to the USAP network.

See detailed information below regarding system requirements, operating system specifications, and the process for computer screening. The following requirements are aligned with the *NSF Computer Security Policy*. Please direct inquiries to the USAP Help Desk at (720) 568-2001 or helpdesk@usap.gov.

*In order to minimize wait time for computer screening, please ensure your system meets the following requirements prior to deployment. Failure to comply with the following guidelines may result in excessive delays or a denial of access. Please be prepared.*

## General System Requirements

► **Administrator Access**

*Obtain Administrator password for personal computers prior to deployment*. Technicians must have the authority to log on to the personal computers at an Administrator level. This enables the screener to accurately review the system configuration and install any necessary patches and antivirus definition files, run screening software, and make any system configuration modifications necessary to provide network connectivity. If an Administrator password is not available, the screening process, as well as the ability to connect to the USAP network and its resources, will be delayed.

► **Connectivity**

All the equipment necessary to connect the computer system to a network must be provided, including the NIC (network interface card), external dongles or attachments used by the NIC, device drivers, etc. All equipment must be in working order.

► **Antivirus**

Administrator ID and password are needed for the antivirus software to update current virus definition files (DAT files). For computers running McAfee antivirus software, the Admin ID and password are needed to configure the software to update automatically from a local USAP server. Raytheon Polar Services Company (RPSC) can provide current DAT files for McAfee and Norton users. All other antivirus software users must ensure proper updates are installed and the computer is virus free prior to deployment. Please note that antivirus software requirements do not apply to computers running a Mac OS X or Linux operating system.

► **Patches**

Computers running Microsoft Windows operating systems must have the ability to be "patched" and include the most current level of the operating system.

► **Client and Server Software**

- Client software used for the purposes of email and web browsing, and other client software, such as SSH and SFTP, are permitted.
- Peer-to-peer (P2P) software, e.g., KaZaA, is not allowed.
- Email server software that provides SMTP/POP port services should not be used.
- Web server software that provides HTTP/HTTPS/FTP services should not be utilized.
- Network management servers, such as DNS and SNMP, should not be running.

## Operating System Specifications

Operating systems have certain criteria that must be met in order to pass the computer screening process. All operating systems should utilize software supported by the operating system vendor. If a user's OS is not in one of the below categories, their connection to the network must be evaluated at a USAP location by an IT technician prior to connecting to the USAP network.

► **Apple**
Mac OS X systems are permitted to connect to the USAP infrastructure at any station. If older Mac OS versions are installed, current antivirus software must also be installed.

► **Linux**
Linux systems/partitions are permitted to connect to the USAP infrastructure at any station. If the computer is configured to dual boot with Microsoft, the Windows partition must comply with the criteria stated below for Microsoft systems.

► **Microsoft**
Ensure the following conditions are met:
- Windows 2000 (Service Pack 4) or XP (SP1 or SP2) and all hot fixes loaded*
- Current antivirus software with latest virus definition files (DAT files)
- Complete/full system virus scan within the previous two weeks
- System32/wins folder does not contain “dllhosts.exe” or “svchosts.exe”

*Microsoft OS service pack and security patch updates are available at www.microsoft.com

## Computer Screening Process

Screening technicians will gather various computer information (see table below), and make it available to all technicians performing screenings on station. Users found using the USAP network without a screening rating of Pass are in violation of IT Security Policy and may be subject to disciplinary action. If possible, computers will be screened during Deployment Orientation for current antivirus software and operating system patches.

► **Deployment Orientation or Christchurch, New Zealand**
Computer screenings during Deployment Orientation or in Christchurch may take anywhere from two hours to a full day. Computers that receive a Pass rating at Orientation/Christchurch within two weeks of deployment may connect to the USAP network upon arrival. A Fail rating indicates the computer must go through remediation before connecting to the USAP network.

► **McMurdo Station or South Pole Station**
Computer screening in McMurdo or South Pole is not required for those computers that have received a Pass rating when screened at other USAP locations within two weeks of deployment. If a computer arrives on station either without being screened or having failed a screening, the owner must contact the McMurdo or South Pole Station Help Desk. IT personnel at McMurdo or South Pole will then perform screening and/or remediation as time allows.

► **Marine Research Vessels (LMG or NBP)**
Screening onboard the Vessels will occur during the port call or within the first two days at sea. IT personnel will perform screening and/or remediation as time allows. Laptops will be returned to their respective owners within 1-2 days.

► **Palmer Station**
Computers arriving at Palmer Station are required to be screened and configured for proper connection to the USAP network. Owners must contact Palmer Station IT personnel prior to connecting to the network. IT personnel will perform screening and/or remediation as time allows.

| **Data Potentially Collected During Computer Screening** | |
|---|---|
| ▪ User name<br>▪ Date of check<br>▪ Computer make and model<br>▪ Computer affiliation (personal, grantee, NSF, other)<br>▪ NSF Tag number (if applicable)<br>▪ Computer hostname<br>▪ OS version<br>▪ OS patch level | ▪ Service pack/service release level<br>▪ Serial number<br>▪ MAC address<br>▪ Wireless MAC address<br>▪ Antivirus software<br>▪ Virus DAT file date<br>▪ Pass (computer cleared to connect to network) or Fail (computer needs remediation) |